WHA GROUP

Policy

นโยบายการจัดการความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

(Cybersecurity and Information Security Management Policy)

การกำกับดูแลและเป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

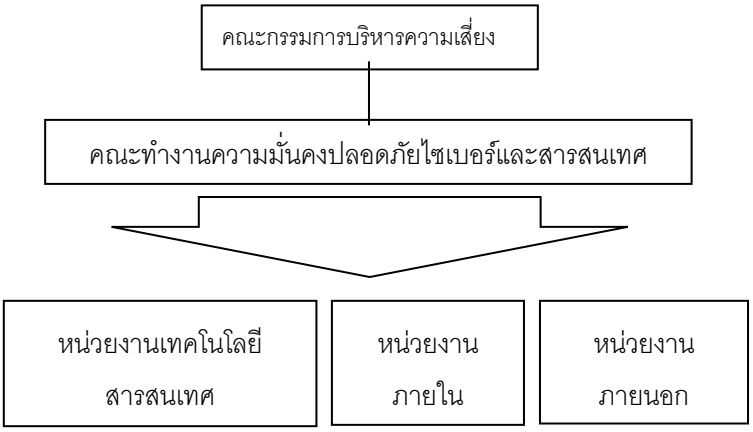
เป้าหมาย

- เพื่อทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบที่เกี่ยวข้องกับข้อมูลให้มีความปลอดภัยด้านสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ ณ ปัจจุบัน และในอนาคตขององค์กร
- เพื่อเตรียมความพร้อมในการรองรับภัยคุกคามทางไซเบอร์ ซึ่งการดำเนินนโยบายนั้นมุ่งเน้นให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (“พ.ร.บ. ไซเบอร์”) นอกจากนี้ทางบริษัทยังให้ความสำคัญในเรื่องการคุ้มครองและเคารพสิทธิในความเป็นส่วนตัวของท่านที่มีอยู่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) และฉบับปรับปรุงแก้ไขตามที่จะมีการปรับปรุงแก้ไขเป็นคราวๆ และกฎหมายและกฎระเบียบที่ใช้บังคับอื่น ๆ ที่ใช้บังคับในประเทศไทย

การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Cybersecurity Governance)

บริษัทฯ ได้ดำเนินการกำกับดูแล และมีการบริหารระบบความมั่นคงปลอดภัยสารสนเทศ ที่สอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 และกรอบความมั่นคงปลอดภัยด้านไซเบอร์ที่ถูกพัฒนาโดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของประเทศสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) และได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ มีการประกาศใช้และถือปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรใน ทุกระดับชั้นขององค์กร ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สิน สารสนเทศขององค์กร

เพื่อให้การจัดการความปลอดภัยสารสนเทศให้เป็นไปอย่างมีระบบและมีความชัดเจน ตั้งแต่ระดับบริหารจนถึง ระดับปฏิบัติการ องค์กรจึงได้จัดทำโครงสร้างความปลอดภัยไซเบอร์และสารสนเทศ รวมถึงการกำหนดบทบาท และหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในองค์กร ลักษณะโครงสร้างของคณะทำงานความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ แสดงดังภาพด้านล่างนี้



โครงสร้างองค์กรของคณะทำงานความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

คณะกรรมการ คณะทำงาน หรือหน่วยงานที่เกี่ยวข้อง	บทบาทหน้าที่และความรับผิดชอบ
คณะกรรมการบริหารความเสี่ยง	- กำหนดนโยบายและกรอบการบริหารความเสี่ยงองค์กร - กำหนดทิศทางกลยุทธ์และเป้าหมาย
คณะทำงานความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ	1) ตรวจสอบ และอนุมัติ ปรับปรุงนโยบายความปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์ 2) วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยให้เข้าใจถึงความปลอดภัยสารสนเทศ

	3) ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ 4) วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่าง ๆ ที่เกิดจากข้อจำกัดของระบบ 5) ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกฉิน
- หน่วยงานเทคโนโลยีสารสนเทศ	- กำหนดระบบ วิธีปฏิบัติ และบริการ ให้แก่ผู้ใช้งานปฏิบัติตาม - ประเมินการติดตามผลงานและรายงานความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงระดับองค์กร
- หน่วยงานภายใน	- ให้การสนับสนุนตามนโยบายความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ - ปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ
- หน่วยงานภายนอก	- ปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

โดยทางบริษัทฯ ได้แต่งตั้งผู้ช่วยกรรมการผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ให้ดำรงตำแหน่ง ประธานคณะทำงานและผู้อำนวยการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) ซึ่งมีหน้าที่ดังต่อไปนี้

(1) เป็นประธานคณะทำงานความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และมีหน้าที่รับผิดชอบด้านความปลอดภัยทางสารสนเทศและเป็นผู้นำในการดำเนินงานทั้งหมดที่เกี่ยวข้องกับความปลอดภัยสารสนเทศในองค์กร

(2) กำหนดเป้าหมาย นโยบายด้านการรักษาความปลอดภัยทางสารสนเทศให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร

(3) เป็นผู้นำเสนอแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการดำเนินงานทางด้านความปลอดภัยสารสนเทศเพื่อขอดำเนินการอนุมัติจากผู้บริหารระดับสูง และเพื่อให้ผู้บริหารระดับสูงมีความตระหนักในความสำคัญในเรื่องความปลอดภัยสารสนเทศ

(4) วิเคราะห์และบริหารความเสี่ยงที่เกี่ยงข้องกับความปลอดภัยทางสารสนเทศ รวมถึงเป็นผู้ประเมินทางเลือกในการรับมือกับความเสี่ยงทางด้านความปลอดภัยทางสารสนเทศอย่างเหมาะสม

(5) จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยทางสารสนเทศ เพื่อให้องค์กรได้มาซึ่งเสถียรภาพความมั่นคงของระบบ ความถูกต้องและการรักษาความลับของข้อมูล

<u>แนวทางและกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ตามมาตรฐาน ISO/IEC 27001:2013</u>

1) ความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY)
2) โครงสร้างความปลอดภัยสารสนเทศ (ORGANIZATION OF INFORMATION SECURITY)
3) ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (HUMAN RESOURCES SECURITY)
4) การบริหารจัดการทรัพย์สิน (ASSET MANAGEMENT)
5) การควบคุมการเข้าถึง (ACCESS CONTROL)
6) การเข้ารหัสข้อมูล (CRYPTOGRAPHY)
7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (PHYSICAL AND ENVIRONMENTAL SECURITY)
8) ความมั่นคงปลอดภัยสาหรับการดำเนินการ (OPERATIONS SECURITY)
9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (COMMUNICATIONS SECURITY)
10) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE)
11) ความสัมพันธ์กับผู้ให้บริการภายนอก (SUPPLIER RELATIONSHIPS)
12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY INCIDENT MANAGEMENT)

13) การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT)
14) ความสอดคล้อง (COMPLIANCE)

แนวทางและกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ตามมาตรฐาน NIST Cybersecurity Framework

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

- END OF DOCUMENT -